ISSN:0975-9646

Sensitive Broadcasting of Data for Cluster Based WSNs

[1]Renuga.A [2]Sakthivel.B

[1]PG Scholar, Department of CSE,
P.S.V. College Of Engineering & Technology, Krishnagiri.
[2]HOD, Department of CSE,
P.S.V. College Of Engineering & Technology , Krishnagiri.

ABSTRACT- Wireless Sensor Networks (WSN) plays vital role in research field. Due to its rapidly increasing application in monitoring various kinds of environment by sensing physical phenomenon. Clustering is an effective way to boost up system performance of the WSNs system. In this project work, we study a secure transmission of data for cluster-based WSNs (CWSNs), where the clusters are formed dynamically and randomly. We propose reliable data Transmission (SET) protocols for CWSNs, called SET-IBOOS, by using the Identity-Based Online/Offline digital Signature (IBOOS) scheme, respectively. SET-IBOOS additionally decreases the computational operating cost for protocol security, which is critical for WSNs, while its defense depends on the stability of the problem of discrete logarithm The results show that the proposed protocols have better performance than the existing secure protocols for CWSNs, in terms of security overhead and energy consumption within time.

Keywords- Cluster-based WSNs, ID-based online/offline digital signature, Energy consumption.

1. INTRODUCTION

Wireless sensor networks (WSNs) refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. WSNs measure environmental conditions like temperature, sound, pollution levels, humidity, wind speed and direction, pressure, etc. WSNs were initially designed to facilitate military operations traffic, and many other consumer and industrial areas. A WSN consists of anywhere from a few hundreds to thousands of sensor nodes.

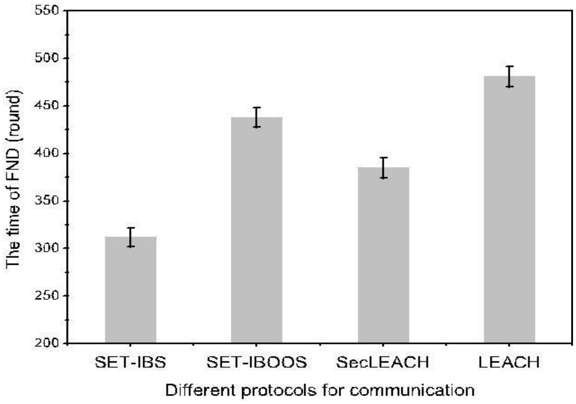
The sensor node equipment includes a radio transceiver along with an antenna, a micro controller, an interfacing electronic circuit, and an energy source, usually a battery. The size of the sensor nodes can also range from the size of a shoe box to as small as the size of a grain of dust. As such, their prices also vary from a few pennies to hundreds of dollars depending on the functionality parameters of a sensor like energy consumption, computational speed rate, bandwidth, and memory.

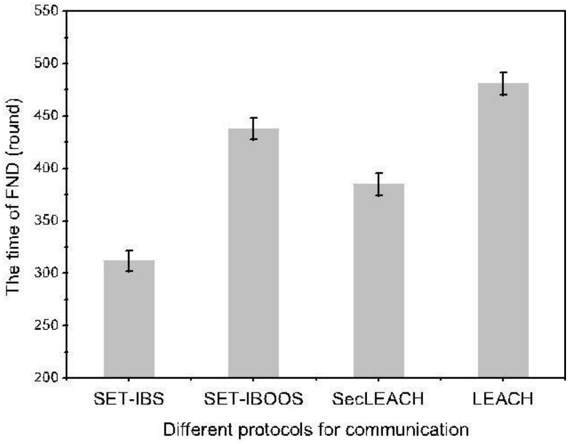
The possibility of the asymmetric key management has been shown in WSNs recently, which compensates the shortage from applying the symmetric key management for security Digital signatures are often used to implement, electronic signature a broader term that refers to any electronic data that carries the intent of a signature, but not all electronic signatures use digital signatures. Digital signatures are among the most basic primitives in cryptography, providing authenticity, integrity, and non-repudiation in an asymmetric key. The identity-based digital signature (IBS) scheme based on the trouble of factoring integers from identity-based Cryptography (IBC), is to derive an entity's public key from its identity information, for example, from its name or ID number. Recently, the concept of IBS has been developed as a key management in WSNs for security Providers often store more than one customer's data on the same server. As a result there is a chance that one user's private data can by viewed by other users (possibly even competitors)The cluster-based hierarchical method. The network is broken into clustered layers, and the data packages travel from a lower cluster head to a higher one, in turn to the BS, for example, [7].

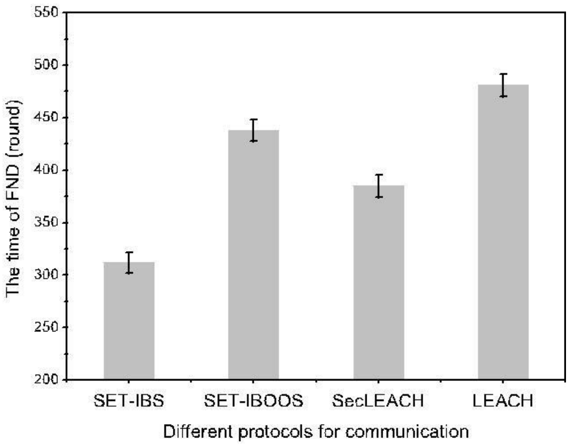
In SET-IBOOS, the offline signature is executed by the CH sensor nodes; thus, sensor nodes do not have to execute the offline algorithm before it wants to sign on a new message. Furthermore, the offline sign phase does not use any sensed data or secret information for signing. This is particularly useful for CWSNs because leaf sensor nodes do not need auxiliary communication for renewing the offline signature.

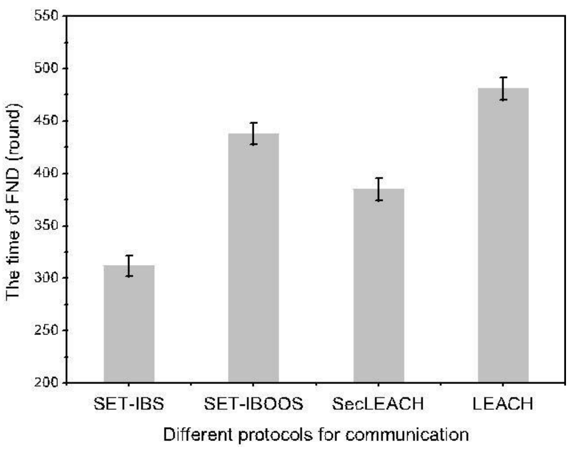
II.RELATED WORK:

Consider a CWSN consisting of a fixed BS and a large number of WSNs, which are same in functionalities and capabilities. We assume that the BS is always dependable i.e., the BS is a trusted authority. The sensor nodes may be damage by attackers, and the data transmission may be interrupted from attacks on wireless channel. In a CWSN, sensor nodes are grouped into clusters, and each cluster has a CH sensor node, which is elected autonomously. Leaf (non-CH) sensor nodes join a cluster depending on the receiving signal strength and transmit the sensed data to the BS via CHs to save energy. The CHs perform data fusion, and transmit data to the BS directly with comparatively high energy. In addition, we assume that all sensor nodes and the BS are time synchronized with symmetric radio channels, nodes are distributed randomly, and their energy is constrained. A sensor node go into sleep mode for energy saving when it does not sense or transmit data, depending on the time-division multiple access (TDMA) control used for data broadcast.









III. PROPOSED SYSTEM

The work is categorized as follows.

A. Protocol Initialization

Generate an encryption key k for the homomorphic encryption scheme to encrypt data messages. Let G be a multiplicative finite cyclic group with order q. The PKG selects a random generator g of group G generation and the master key will be generated randomly. Private key will be generated to each node automatically.

B. SET-IBOOS protocols

Neighborhood authentication used for secure access and data transmission to nearby sensor nodes. Storage cost represents the requirement of the security keys stored in sensor node's memory. Network scalability indicates whether a security protocol is able to scale without compromising the security requirements the larger network scale increases, the more orphan nodes appear in the network, and vice versa[2].Communication overhead. the security overhead in the data packets during communication .Computational overhead the energy cost and compu-tation efficiency on the generation and verification of the certificates or signatures for security.

C. Message Size of Data Transmission

In this part, we do the quantitative calculation of the message packet size on data transmission in the steady state (main phase) of the different protocols for comparison.
Although most of existing WSNs constructed in real-world use no more than 200 nodes [1], a large scale WSN could consist of hundreds of nodes or more in the future. Thus in this paper, we set the length of node IDs as 2 bytes. . For example, when using the Tate pairing [15] for elliptic curve cryptography (ECC), the order q of G1 and G2 could be a 160-bit prime, if the required security level of ECC is equivalent to RSA with 1,024-bit keys (RSA-1,024) [5], which provides the currently accepted security level. In this way, the total message size of a data packet is 64 bytes in SET-IBOOSS. Moreover, p could be a 512-bit prime to achieve higher level of security.

D. SOLUTIONS TO ATTACKS

The passive adversaries cannot decrypt the eavesdropped message without the decryption key. SET-IBOOS are resilient and robust to the sinkhole and selective forwarding attacks because the CHs being attacked are capable to ignore all the communication packets with bogus node IDs or bogus digital signatures. Together with round-rotating mechanism and digital signature schemes, SET-IBS and SET-IBOOS are resilient to the HELLO flood attacks involving CHs.

IV. CONCLUSION

In this paper, we first reviewed the data transmission issues and the security issues in CWSNs. The deficiency of the symmetric key management for secure data transmission has been sloved and reliable data broadcasting with less computation overhead and also less energy consumption during data transmission.

ACKNOWLEDGEMENT

Our sincere thanks to our honorable Chairman **Dr.P.Selvam M.A., B.Ed., M.Phil., Ph.D.,** P.S.V College Of Engineering & Technology, Krishnagiri for giving this opportunity. We express my profound gratefulness to our Secretary **Mr.S.Vivek M.A., M.B.A.,** and our Principal **Dr.K.Rangasamy M.E., M.B.A., Ph.D.,** P.S.V College of Engineering & Technology. My special thanks to **Prof.B.Sakthivel M.E.,** HOD/CSE for their guidance and continuous motivation in publishing technical papers. Last but not the least I thank my parents for their valuable support & encouragement.

REFERENCES

[1] F. Hess, "Efficient Identity Based Signature Schemes Based on Pairings," Proc. Ninth Ann. Int'l Workshop Selected Areas in Cryptography (SAC), pp. 310-324, 2003.

[2] J.J. Rotman, An Introduction to the Theory of Groups, fourth ed. Springer-Verlag, 1994.

[3] K.S. McCurley, "The Discrete Logarithm Problem," Proc. Symp. Applied Math., Programming Computer Science, vol. 42, pp. 49-74, 1990.

[4] D. Boneh, I. Mironov, and V. Shoup, "A Secure Signature Scheme from Bilinear Maps," Proc. RSA Conf. The Cryptographers' Track (CT-RSA), pp. 98-110, 2003.

[5] P. Barreto et al., "Efficient Algorithms for Pairing-Based Crypto-systems," Proc. 22nd Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 354-369, 2002.

[6] C. Castelluccia, E. Mykletun, and G. Tsudik, "Efficient Aggrega-tion of Encrypted Data in Wireless Sensor Networks," Proc. Second Ann. Int'l Conf. Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous), pp. 109-117, 2005.

[7] H. Lu, J. Li, and G. Wang, "A Novel Energy Efficient Routing Algorithm for Hierarchically Clustered Wireless Sensor Net-works," Proc. Fourth Int'l Conf. Frontier of Computer Science and Technology (FCST), pp. 565-570, 2009.

[8] Y. Jia, L. Zhao, and B. Ma, "A Hierarchical Clustering-Based Routing Protocol for Wireless Sensor Networks Supporting Multiple Data Aggregation Qualities," IEEE Trans. Parallel & Distributed Systems, vol. 4, nos. 1/2, pp. 79-91, 2008.

[9] J. Liu et al., "Efficient Online/Offline Identity-Based Signature for Wireless Sensor Network," Int'l J. Information Security, vol. 9, no. 4, pp. 287-296, 2010.

[10] H. Lu, J. Li, and H. Kameda, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using ID-Based Digital Signature," Proc. IEEE GLOBECOM, pp. 1-5, 2010.

[11] B. Sun et al., "Intrusion Detection Techniques in Mobile Ad Hoc and Wireless Sensor Networks," IEEE Wireless Comm. Magazine, vol. 14, no. 5, pp. 56-63, Oct. 2007.

[12] D.W. Carman, "New Directions in Sensor Network Key Manage-ment," Int'l J. Distributed Sensor Networks, vol. 1, pp. 3-15, 2005.

[13] K.S. McCurley, "The Discrete Logarithm Problem," Proc. Symp. Applied Math., Programming Computer Science, vol. 42, pp. 49-74, 1990.

[14] D. Boneh, I. Mironov, and V. Shoup, "A Secure Signature Scheme from Bilinear Maps," Proc. RSA Conf. The Cryptographers' Track (CT-RSA), pp. 98-110, 2003.

[15] P. Barreto et al., "Efficient Algorithms for Pairing-Based Crypto-systems," Proc. 22nd Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 354-369, 2002.

BIOGRAPHIES

Ms.A.RENUGA received her **B.E.** degree in Computer Science and Engineering from Anna University, Chennai, Tamilnadu, in 2011, Currently, she is pursuing **M.E.** degree in P.S.V. College of Engineering and Technology, Krishnagiri, Tamilnadu, affiliated to Anna University, Chennai, Tamilnadu. She has two international publications and her area of interests are Cloud Computing and Security. She has two international publications.

PROF.B.Sakthivel received his **B.Tech** Computer Science and Engineering from MNNIT, **M.E** degree from VMKV University. At present he is working as HOD of CSE Department at P.S.V College Of Engineering and Technology, Krishnagiri, Tamilnadu, affiliated to Anna University Chennai. He has published papers in National and International journals. He wrote a book on Data Structures & Algorithms. His teaching and research areas include Data Structure & Algorithm, Network Secur